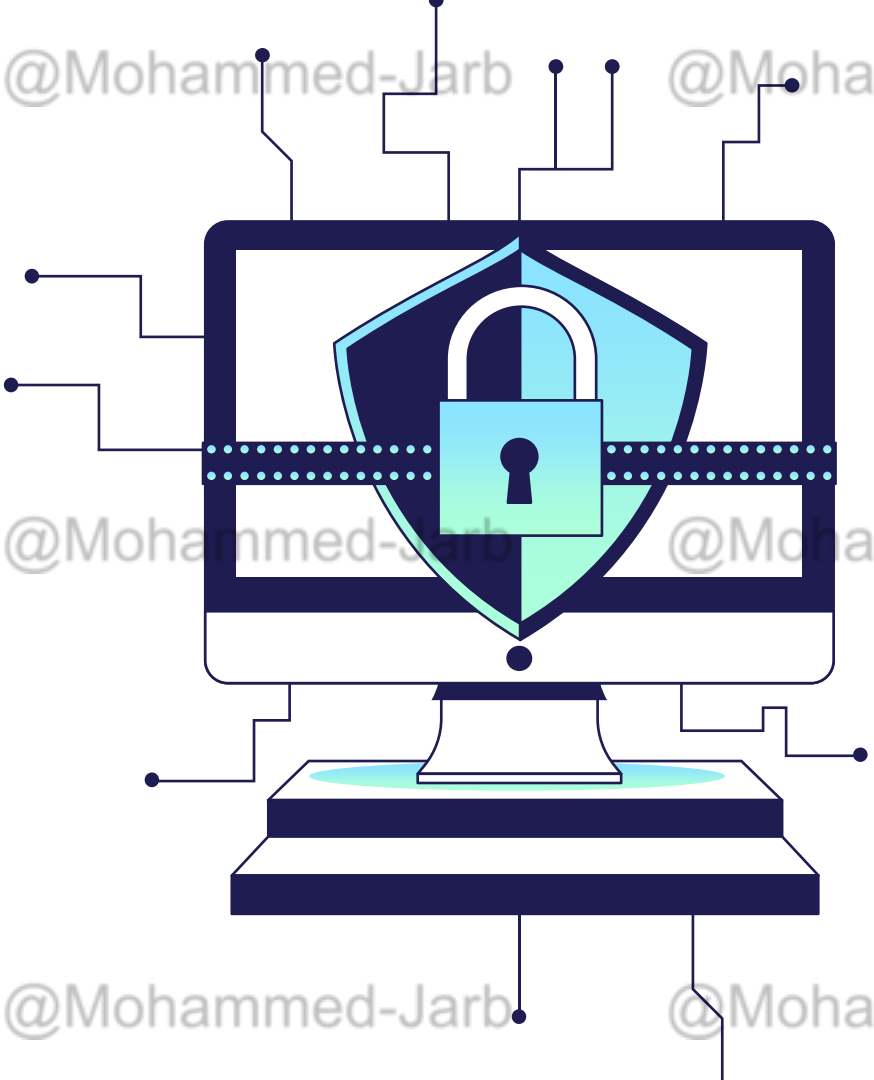


الهندسة الاجتماعية

مفهوم والأهمية والأساليب وطرق الحماية

الهندسة الاجتماعية

تعريف

هي ممارسة يستخدم فيها المهاجمون تقنيات التلاعب النفسي لخداع الأفراد وإقناعهم بالقيام بأفعال معينة أو الكشف عن معلومات حساسة, تعتمد هذه الطريقة على استغلال نقاط الضعف البشرية، مثل الثقة والفضول

• المهندسون الاجتماعيون يستخدمون طرقًا متقنة لإقناع الضحايا باتخاذ إجراءات غير عادية، مثل النقر على روابط مشبوهة أو إرسال معلومات حساسة أو إرسال أموال.

• رسائل البريد الإلكتروني تعد وسيلة شائعة وخطيرة للهندسة الاجتماعية، حيث يمكن تخصيصها لتبدو موثوقة وتحتوي على عناصر يمكنها خداع الضحية.

• الهندسة الاجتماعية ليست محمية بأدوات أمان مصممة لحماية المستخدمين، وبالتالي فإن الوعي والحذر يلعبان دورًا مهمًا في تجنب الوقوع في فخاخها.

أهمية الهندسة الاجتماعية

يجب ان تكون على رأس قائمة وسائل الهجوم التي يجب أن نحاول حماية المعلومات منها وذلك لأن...

١- تعد من الطرق الأكثر فعالية التي يلجأ إليها المهاجمون بسبب بساطتها وفعاليتها مقارنةً بالتقنيات الأخرى المعقدة

٢- غالبًا ما يتم إهمال خطر الهندسة الاجتماعية من قبل متخصصي أمن المعلومات ومستخدمي الكمبيوتر ، مما يجعل المعلومات الشخصية أكثر عرضة للخطر.

جوانب الهجمات بأسلوب الهندسة الاجتماعية

– الجانب الحسي

حيث يكون التركيز على موضع الهجوم والبيئة المحية به مثل

مكان العمل

يتظاهر المهاجم أنه أحد الموظفين وإذا تمكن من الدخول فأنه يطوف بالمكاتب لجمع كلمات المرور او تثبيت برمجيات ضارة في الأجهزة او لأي غرض اخر

الهاتف

يستخدم لشن الهجمات , فقد يتصل المهاجم بمركز تقديم الدعم الفني ويطلب بعض المعلومات الفنية حتى يحصل على ما يريده مثل كلمات المرور وغيرها

الإنترنت

عندما يستخدم شخص نفس كلمة المرور في جميع المواقع , ينشئ المهاجم صفحة إنترنت يقدم خدمات معنية مثل تنزيل البرامج مجانا ويطلب من المستخدم ادخال اسم مستخدم وكملة مرور ويحاول المهاجم الدخول الى حساباته باستخدام كلمة المرور التي ادخلها

– الجانب النفسي

يتمحور حول بناء ثقة مصطنعة لإقناع الضحية بأن المهاجم مخول بالوصول للمعلومات الخاصة

أسلوب الإقناع

١- طريقة الاقناع المباشرة : هو عندما يقدم الشخص حججه وأدلته بوضوح، مستخدمًا اللغة الصريحة والمباشرة لإقناع الآخرين بفكرة معينة أو لاتخاذ إجراء محدد

٢- طريقة الاقناع الغير مباشرة : هو عندما يستخدم الشخص أساليب أكثر دقة وتلميحًا مثل القصص المجاملات، أو الربط العاطفي لتحريك الآخرين نحو فكرة أو إجراء دون طرح الحجج بشكل مباشر

أساليب الاقناع

– الاقناع المباشر

01 الهجوم عبر البريد الإلكتروني

حيث يتم إرسال رسالة إلكترونية تطلب بشكل مباشر من الضحايا تقديم بيانات تسجيل الدخول الخاصة بهم، مدعية أن هناك مشكلة مع حساباتهم تتطلب تحققًا فوريًا

02 مكالمات الدعم الفني الاحتيالية

يدعي المهاجم أنه ممثل لخدمة عملاء شركة معروفة ويطلب مباشرة من الضحية تزويده بمعلومات حساسة، مثل كلمات السر أو البيانات المالية، لحل مشكلة وهمية

03 التهديدات والإكراه

يستخدم المهاجم تكتيكات التخويف، مثل التهديد بالملاحقة القانونية أو التأثير على الائتمان المالي، ليجبر الضحية على تقديم المعلومات الحساسة بشكل مباشر وتحت ضغط

– الاقناع غير المباشر

01 تمويه الهوية بزي السلطة

يرتدي المهاجم زيًا يوحي بأنه شخص صاحب سلطة، مثل ضابط شرطة أو مدير شركة، ليكسب ثقة الضحية ويشجعها على الكشف عن المعلومات الحساسة

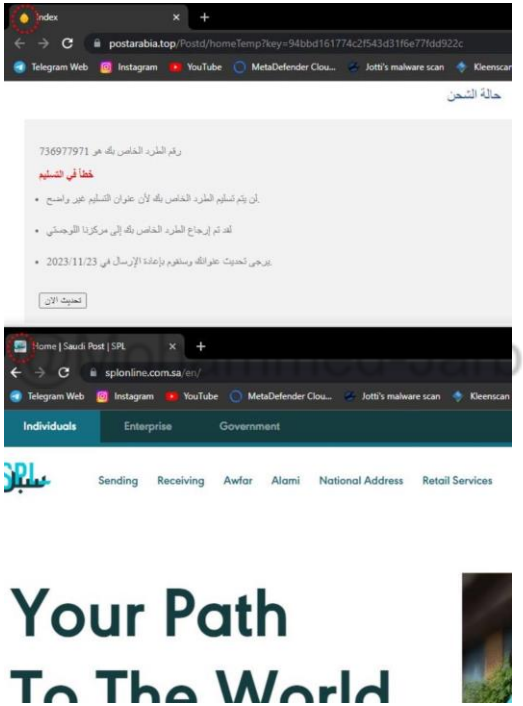
02 الإغراء بامتلاك شيء نادر

مثل وعد بالحصول على برمجيات حصرية أو دعوة للانضمام إلى خدمة محدودة، لتحفيز الضحية على الكشف عن بياناتها الشخصية أو المالية

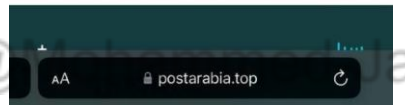
03 رد الجميل

يعتمد على منح شيء ذو قيمة أو تقديم معروف أولاً، مما يخلق لدى الشخص الآخر شعورًا بالالتزام لتقديم شيء في المقابل

مثال من واقع الحياة



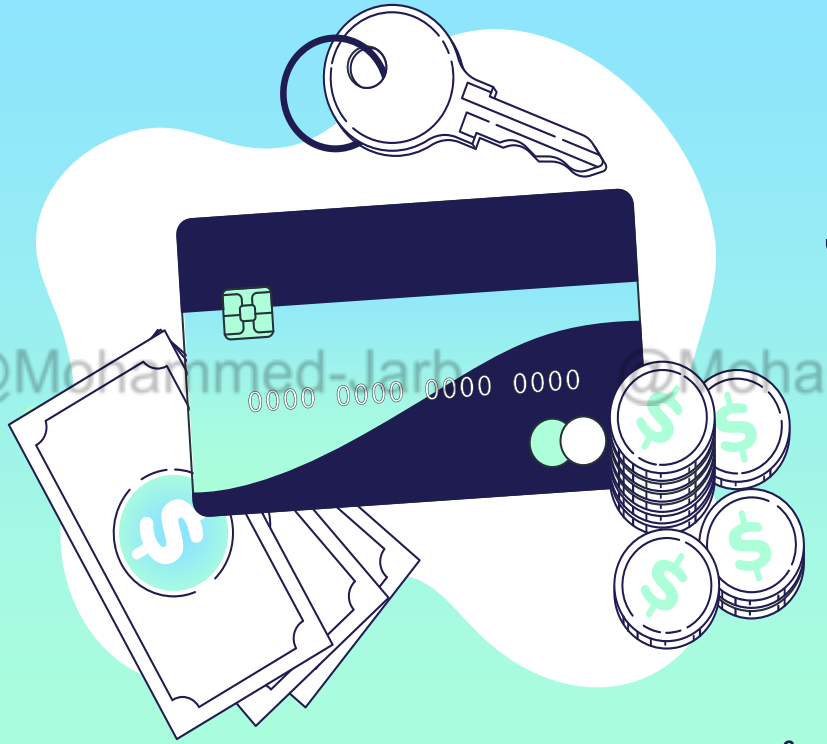
استخدم المهاجم حيلة ذكية وهي عند النقر على دخول او الفروع سيتم تحويلك الى موقع سبل الأصلي لتنجب الشبهة



نلاحظ الفروقات بين الموقع الأصلي والموقع المزيف الذي أرسله المهاجم

يستخدم هذا المهاجم الاقناع المباشر ونلاحظ انه يطلب من المستخدم تحديث العنوان وأيضا نلاحظ ان المرسل يستخدم بريد غير تابع لجهة سبل والرابط مريب

نصائح لتجنب الوقوع في حيل المهاجمين



التحقق المستمر

1

دائمًا قم بالتحقق من هوية الشخص أو الكيان الذي يطلب المعلومات، خاصة إذا كانت الطلبات تأتي عبر قنوات غير رسمية مثل البريد الإلكتروني أو الهاتف. لا تتردد في الاتصال بالشركات أو الأشخاص مباشرة عبر قنوات التواصل المعترف بها للتأكد من صحة الطلبات

الوعي التعليمي

2

تثقيف نفسك والموظفين حول أنواع مختلفة من هجمات الهندسة الاجتماعية وكيفية العمل في حال التعرض لها يشمل ذلك فهم العلامات الدالة على محاولات الاحتيال، مثل الأخطاء الإملائية في الرسائل البريدية أو طلبات المعلومات المفاجئة وغير المتوقعة

استخدام تقنيات التحقق المتعدد

3

تفعيل واستخدام وسائل التحقق متعدد العوامل لجميع الحسابات الإلكترونية الهامة، مما يضيف طبقة أمان إضافية ويقلل من فرص نجاح الهجمات التي تعتمد على سرقة البيانات الحساسة من خلال الهندسة الاجتماعية

الخلاصة

الهندسة الاجتماعية هي إعمال الحيل النفسية لخداع مستخدمي الحاسوب للوصول إلى المعلومات المخزنة فيها, وهي أسهل الأساليب وأكثرها فعالية لأنها تهاجم العنصر البشري الذي هو أضعف نقطة في منظومة حماية المعلومات, ولذا يجب ان تكون على رأس قائمة المعنيين بحماية المعلومات.